CS276: Cryptography September 10, 2015

PRGs and PRFs

Instructor: Alessandro Chiesa *Scribe: Pratyush Mishra*

1 Pseudorandom Generator

Recall that the definition of a pseudorandom generator from prior lectures:

Definition 1 *A PRG with output l is a deterministic polynomial time algorithm* G *such that:*

1. $|\mathsf{G}(1^k, s)| = l(|s|)$
2. $\mathsf{G}(1^k, U_k)$ *is pseudorandom, i.e.* $\left\{\mathsf{G}(1^k, U_k)\right\} \stackrel{c}{=} \left\{U_{l(k)}\right\}_k$.

We then saw how to construct a pseudorandom generator from a one-way permutation to get a PRG with a one-bit expansion. Now, we will first look at the pseudorandomness of several invocations of a PRG on independent seeds, and will then see how to construct a PRG with polynomial expansion.

2 PRGs on Independent Seeds

To begin this construction, we first prove a lemma on the pseudorandomness of the concatenation of invocations of a PRG G on independent seeds:

Lemma 2 *If* $\mathsf{G} : \{0,1\}^n \to \{0,1\}^m$ *is a PRG, then so is*

$$\vec{\mathsf{G}}(\vec{s}) = (\mathsf{G}(s_1), \ldots, \mathsf{G}(s_p)) \, \forall \text{ poly } p$$

Proof:

For contradiction, assume $\exists$ ppt. D such that

$$\delta(k) = \left| Pr\left[D(\vec{\mathsf{G}}(U_{np})) = 1\right] - Pr\left[D(U_{mp}) = 1\right] \right|$$

is negligible in k. Then, for each i, define

$$H_k^{(i)} = \left(\mathsf{G}\left(U_n^{(1)}\right), \cdots, \mathsf{G}\left(U_n^{(i)}\right), U_m^{(i+1)}, \cdots, U_m^{(p)}\right)$$

Note that $H_k^{(0)} = U_{mp}$, and $H_k^{(p)} = \mathsf{G}(\vec{U}_{np})$. Then, by the hybrid argument, we know that there exists i such that:

$$\left| Pr\left[D(H_k^{(i)}) = 1\right] - Pr\left[D(H_k^{(i+1)}) = 1\right]\right| \geq \frac{\delta(k)}{p(k)}$$

Now we construct D' to distinguish between $\mathsf{G}(U_n)$ and U_m.

Algorithm 1: Distinguisher for $\mathsf{G}(U_n)$ and U_m.

1: **Machine** $D'(y)$
2: $y_1, \cdots, y_i \xleftarrow{\$} \mathsf{G}(U_n)$
3: $y_{i+2}, \cdots, y_{p(k)} \xleftarrow{\$} U_m$
4: $\vec{y} = (y_1, \cdots, y_i, y, y_{i+2}, \cdots, y_{p(k)})$
5: **Output** $D(\vec{(y)})$

If $y \sim \mathsf{G}(U_n)$, we have $\vec{y} \sim H_k^{(i+1)}$. Else if $y \sim U_m$, we have $\vec{y} \sim H_k^{(i)}$.

Therefore, D' distinguishes with probability $\dfrac{\delta(k)}{p(k)}$, which is non-negligible in k. □

Now, we can proceed to construct a PRG with an larger expansion factor.

3 Increasing the Expansion Factor

Now, we look at constructing a PRG that has a polynomial expansion factor.

Theorem 3 *Let* G *be a PRG with* $l(k) = k + 1$*, i.e. one bit expansion. Then,* $\forall p \; \exists$ *PRG* $\overline{\mathsf{G}}$ *with* $l(k) = p(k)$*.*

Proof:

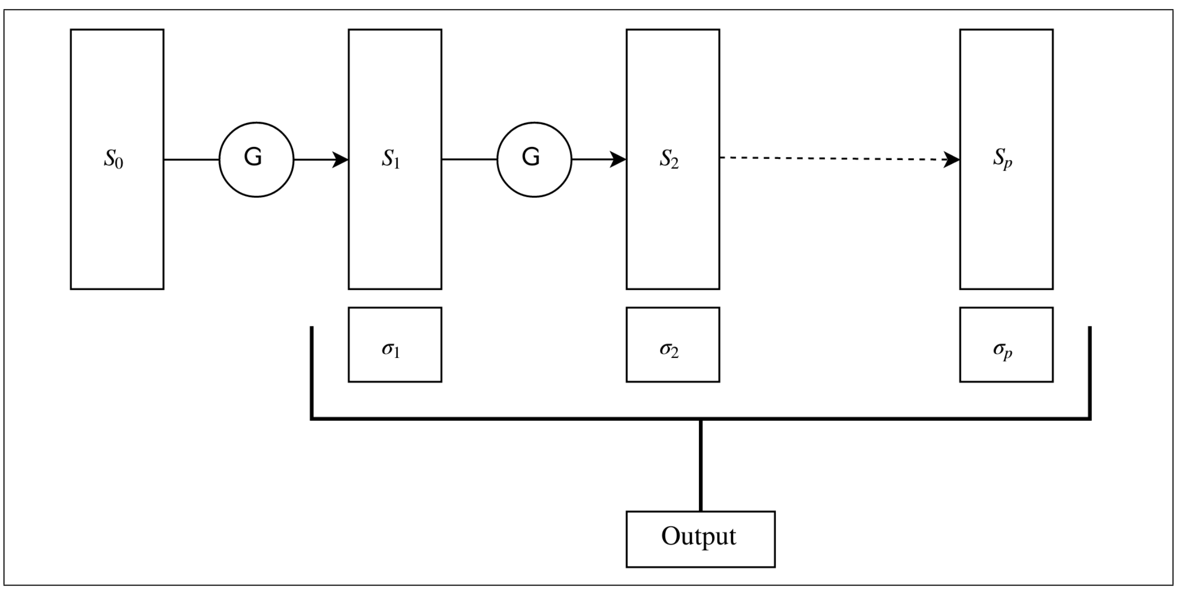

Figure 1: Construction of $\overline{\mathsf{G}}$

In Figure 1 , we see the construction of $\overline{\mathsf{G}}$. Formally, we have

$$\overline{\mathsf{G}}(s) = \mathsf{G}^{(p)}(s)$$

where $\mathsf{G}^{(i)}(s) = b||\mathsf{G}^{(i-1)}(x)$ and $\mathsf{G}(s) = x||b$.

Now assume for contradiction that $\overline{\mathsf{G}}$ is not a PRG. Therefore, $\exists$ ppt. D such that

$$\delta(k) = \left| Pr\left[D(\overline{\mathsf{G}}(U_k)) = 1\right] - Pr\left[D(U_p) = 1\right]\right|$$

is non-negligible in k.

Then, for each i, we define

$$H_k^{(i)} = U_{p-i}||\mathsf{G}^{(i)}(U_k)$$

Note that $H_k^{(0)} = U_p$ and $H_k^{(p)} = \overline{\mathsf{G}}(U_k)$. Now once again by the hybrid argument, there exists a i such that

$$\left| Pr\left[D(H_k^{(i)}) = 1\right] - Pr\left[D(H_k^{(i+1)}) = 1\right]\right| \geq \frac{\delta(k)}{p(k)}$$

Now, we can define a distinguisher for G:

Algorithm 2: Distinguisher for $\mathsf{G}(U_k)$ and U_{k+1}.

Machine $D'(z)$
- $b_1, \cdots, b_{p-i-1} \stackrel{\$}{\leftarrow} U_1$
- $b_{i+2}, \cdots, b_{p(k)} \stackrel{\$}{\leftarrow} \mathsf{G}^{(i)}(z)$
- $\vec{b} = (b_1, \cdots, b_{p(k)-i-1}, b_{p(k)-1}, \cdots, b_p)$
- **Output** $D(\vec{(y)})$

If $z \sim \mathsf{G}(U_k)$, we have $\vec{b} \sim H_k^{(i+1)}$. Else if $z \sim U_{k+1}$, we have $\vec{b} \sim H_k^{(i)}$.

Therefore, D' is a distinguisher for G with advantage $\dfrac{\delta(k)}{p(k)}$, which is non-negligible in k. This is not possible, and hence $\overline{\mathsf{G}}$ is a a PRG. $\square$

4 Pseudorandom Functions

A pseudorandom function is called so if it cannot be distinguished from a random function by an efficient observer. More formally, we define this primitive using ”Oracle Indistinguishability”.

Definition 4 *A function ensemble is* $\mathcal{F} = \{\mathcal{F}_k\}_k$ *where* $\mathcal{F}_k$ *is a distribution over functions* $f\colon \{0,1\}^k \to \{0,1\}^k$.

Definition 5 *The uniform function ensemble is* $\mathcal{U} = \{\mathcal{U}_k\}_k$ *where* $\mathcal{U}_k$ *is the uniform random distribution over functions* $f\colon \{0,1\}^k \to \{0,1\}^k$.

Definition 6 *A function ensemble is efficiently computable if* $\exists$ *ppt sampler* S *and deterministic poly-time evaluator* E *such that:*

1. $S(1^k) = \mathcal{F}_k$
2. $\forall f \in \mathcal{F}_k, E(1^k, f, x) = f(x)$

Definition 7 $\mathcal{X}$ *is pseudorandom if* $\mathcal{X} \stackrel{c}{=} \{\mathcal{U}\}_{l(k)}$*. That is,* $\forall$ *ppt* D, $\left|Pr\left[D(\mathcal{X}_k) = 1\right] - Pr\left[D(\mathcal{U}_{l(k)}\right]\right|$ *is negligible in* k.

Definition 8 *A function ensemble* $\mathcal{F}$ *is pseudorandom if* $\forall$ *ppt* D*:* $\left|\underset{f\in\mathcal{F}}{Pr}\left[D^f(\mathcal{X}_k) = 1\right] - \underset{u\in\mathcal{U}_k}{Pr}\left[D^u(\mathcal{U}_{l(k)}) = 1\right]\right|$ *is negligible in* k

Definition 9 $\mathcal{F}$ *is a PRF if it is efficient and pseudorandom.*

Theorem 10 *The existence of a PRG with* $2\times$ *expansion implies the existence of PRFs.*

Proof Intuition: Let G be such a PRG. Let $\mathsf{G}_0 = \mathsf{G}(s)[0..k-1]$ and $\mathsf{G}_1 = \mathsf{G}(s)[k..2k-1]$. Now, $\mathsf{G}(U_k) \stackrel{c}{=} U_{2k}$ and $\mathsf{G}_0(U_k) \stackrel{c}{=} U_k \stackrel{c}{=} \mathsf{G}_1(U_k)$.

Furthermore, we have that $(\mathsf{G}_0 \circ \mathsf{G}_1)(U_k) \stackrel{c}{=} U_k \stackrel{c}{=} (\mathsf{G}_1 \circ \mathsf{G}_0)(U_k)$.

Now, to double once again, we have: $(\mathsf{G}_1 \circ \mathsf{G}_0)(U_k)||\mathsf{G}_1(U_k) \stackrel{c}{=} U_{2k}$. To get quadruple expansion, we create $(\mathsf{G}_0 \circ \mathsf{G}_0)(U_k)||(\mathsf{G}_0 \circ \mathsf{G}_1)(U_k)||(\mathsf{G}_1 \circ \mathsf{G}_0)(U_k)||(\mathsf{G}_1 \circ \mathsf{G}_1)(U_k) \stackrel{c}{=} U_{4k}$. Thus we take a 2 bit seed into an expoentially larger output. This is the template for our construction.